## REMARKS/ARGUMENTS

This Amendment is in response to the Final Office Action dated May 20, 2005. Claims 1-32 are pending. Claims 1, 7, 12, 16, and 22 have been amended, and claims 3-6 and 17-21 have been canceled. Accordingly, claims 1-2, 7-16, and 22-32 remain pending in the present application.

This Amendment is submitted in accordance with Rule 116 in an earnest effort to put the application in better condition for allowance. It is believed that Applicant's response has not amended the claims in a way that would raise new issues for consideration or that would require further searching of the prior art on the part of the Examiner. Arguments are also presented below that Applicant believes should render the claims allowable. In the event, however, that the Examiner is not persuaded by the arguments, it is respectfully requested that the Examiner enter the Amendment to clarify issues upon appeal.

Attorney for the Applicant thanks Examiner Dada for the telephone interview on July 18, 2005 in which the differences between the claims of the present invention and the cited prior art references were discussed. In response to the interview, independent claim 1 has been amended to incorporate the limitations of canceled claims 3-6, and independent claim 16 has been amended to incorporate the limitations of canceled claims 17-21. Claims 12 and 22 have been amended to correct claim dependencies errors. No new matter has been entered.

The Examiner rejected claims 1-32 under 35 USC §103(a) as being unpatentable over Scott et al. (US publication number 2002/0049760) in view of Farber et al. (US patent number 5,978,791). Applicant respectfully disagrees.

As discussed during a telephone interview, it is unclear to the Applicant why or how Farber could be used to modify Scott given the differences in the two systems. Scott is a peer-to-peer system in which copies of the same files are transferred among the peers. To eliminate the fact that the same file can have different file names, Scott associates with each file a fingerprint ID relating to its file content. In contrast, Farber teaches a multiprocessor system in which the processors can be configured in a peer-to-peer arrangement. Based on the content of a file, Farber assigns a True Name to the file so that the system can store at most one copy of the data item at any given location, even when multiple data names in the system referred to the same content. Storing only one copy of a file is opposite to a traditional peer-to-peer file sharing arrangement in which multiple copies of the same files are shared between the peers.

Second, both Scott's fingerprint and Farber's True Name establish a unique data identifier for a particular file based on the content of the file using hash and message digest functions, such as MD and SHA. Therefore, even if Scott and Farber were combined, despite the above, it is unclear how the teaching of Farber could be used to augment or modify the teaching of Scott with respect to Scott's fingerprint function.

Nevertheless, it is respectfully submitted that the combination of Scott and Farber fail to teach or suggest the claims of the present invention for several reasons.

*The Scott and Farber combination fails to teach or suggest publisher authentication.*

The claims of the present invention provide a method and system for electronically delivering files in a peer-to-peer network that enables secure and reliable peer-to-peer file sharing between two client nodes. The authenticity of the publisher in

the present invention is established by incorporating publisher information in the fingerprint. As described in the specification, each user of the P2P network is required to register with the network, and account information is generated for the user including a digital certificate that includes a public key and a private key. When the user publishes a file, a bitstream ID is generated for the file, and the user's private key is used to generate a digital signature for the file. In one embodiment, the bitstream ID 34, the file information, and the digital signature 40 form the fingerprint for the file. The fingerprint ensures that the file is transmitted in its original state (data integrity) by the identified user/publisher (page 10, line 20 through page 11, line 8).

Neither Scott or Farber disclose using public/private key encryption and assigning a private key to each user of a peer-to-peer network, using the private key to create a digital certificate, using the digital certificate to generate a fingerprint for each file when the file is published, and then generating a new fingerprint by the client nodes upon receipt of the file "to determine the authenticity of the file and publisher.

More specifically, the combination of Scott and Farber fails to teach or suggest "generating account information for a user, including a digital certificate, in response to a registration process, wherein the digital certificate includes a private key and a public key;" "generating a bitstream ID for the file and including the bitstream ID in the fingerprint;" "using the private key to generate a digital signature from the file and including the digital signature in the fingerprint;" and "authenticating the file by generating a new bitstream ID and comparing the new bitstream ID to the bitstream ID in the fingerprint stored on the server, and using the user's public key to decrypt the digital signature," as recited in claims 1 and 16.

Further, the combination of Scott and Farber fails to teach or suggest using the

fingerprint/True Name to "determine the authenticity of... *the publisher*," as recited. Scott's stated purpose for generating the fingerprint ID is "to identify identical files stored in a peer-to-peer network which have different filenames and/or other metadata descriptors, and to use the fingerprint ID to retrieve the desired content from one or more of the identified files [0008]. Farber's stated purpose for generating the True Name is to identify "a data item in the system, where the identity of the data item depends on all the data in the data item and only on the data in the data item" (col. 1, lines 28-34). Thus, the combination of Scott and Farber fails to teach or suggest using the fingerprint or True Name to determine the authenticity of the "publisher" of the file, as recited in claims 1, 16, 31, and 32.

In the rejection of claims in 3 and 18, the Examiner took Official notice that it is well-known in the art to generate a digital certificate that includes a private key and a public key. Although this may be, digital certificates are typically used for encrypting data for security reasons. The Examiner has failed to cite any art that teaches or suggests the incorporation of a digital certificate of a publisher into a fingerprint for a file so that client nodes in a peer-to-peer network can determine the authenticity of the publisher when the file is transferred from node to another node. Absent any teaching or suggestion to the contrary, it is believed claims 1, 16, 31, and 32 are allowable over the cited references.

*Scott and Farber fail to teach or suggest performing authentication on a second client node by generating a new fingerprint and comparing the new fingerprint to the fingerprint stored on the server*

The Examiner admits that Scott fails to teach or suggest generating a new

fingerprint for the file and comparing the new fingerprint with the fingerprint on the server node to determine the authenticity of the file and publisher. The Examiner cited Farber for teaching this step.

Farber, however, also fails to teach or suggest generating either a new fingerprint or bitstream ID in the fingerprint for a file after the file is transferred from "the first client node directly to the second client node", where the new fingerprint or bitstream ID is compared with the original fingerprint or bitstream ID stored on the server to determine the authenticity of the file and publisher, as recited in the claimed invention.

The Examiner cites Farber column 12, lines 54-67 through column 13, lines 1-18 for teaching these features. However, this passage of Farber only states:

> 1. Calculate True Name
>
> A True Name is computed using a function, MD, which reduces a data block B of arbitrary length to a relatively small, fixed size identifier, the True Name of the data block, such that the True Name of the data block is virtually guaranteed to represent the data block B and only data block B.
>
> The function MD must have the following properties:
>
> 1. The domain of the function MD is the set of all data items. The range of the function MD is the set of True Names.
> 2. The function MD must take a data item of arbitrary length and reduce it to an integer value in the range 0 to N-1, where N is the cardinality of the set of True Names. That is, for an arbitrary length data block B, 0.ltoreq.MD(B).ltoreq.N.
> 3. The results of MD(B) must be evenly and randomly distributed over the range of N, in such a way that simple or regular changes to B are virtually guaranteed to produce a different value of MD(B).
> 4. It must be computationally difficult to find a different value B' such that MD(B)=MD(B').
> 5. The function MD(B) must be efficiently computed.
>
> A family of functions with the above properties are the so-called message digest functions, which are used in digital security systems as techniques for authentification of data. These functions (or algorithms) include MD4, MD5, and SHA.
>
> In the presently preferred embodiments, either MD5 or SHA is employed as the basis for the computation of True Names. Whichever of

> these two message digest functions is employed, that same function must be employed on a system-wide basis.
>
> It is impossible to define a function having a unique output for each possible input when the number of elements in the range of the function is smaller than the number of elements in its domain. However, a crucial observation is that the actual data items that will be encountered in the operation of any system embodying this invention form a very sparse subset of all the possible inputs.

As can be seen, the cited passage of a Farber only describes the mechanism by which a True Name is calculated for a data item or file using algorithms such as MD or SHA. Nothing in the description for the True Name primitive, or any other of the primitive mechanisms, teaches or suggests that once a file is transferred from one client node to another in a peer-to-peer network, that the client node to which the file is transferred generates a *new* fingerprint/True Name for the file and then *compares* it with the fingerprint/True Name stored on a server, as recited in claims 1, 16, 31, and 32.

*Scott and Farber fail to teach subscription services*

Referring now to claims 2, 17, 31, and 32, it is respectfully submitted that a combination of Scott and Farber also fails to teach or suggest "enabling subscription-based decentralized file downloads," as claimed. The Examiner cited Scott, page 4, paragraphs [0046]-[0049] and page 3, paragraph [0034] for teaching subscription-based decentralized file downloads. As described below, however, the cited paragraphs fail to disclose such.

Paragraph [0046] describes the process of a requesting peer choosing a file to download from a list of locations; paragraph [0047] describes that once the requesting peer has chosen a first location to start retrieving the file from (e.g., peer2) the requesting peer makes a request operation to the second peer for file that has a

.desired hash ID, and the requesting peer transmits the contents of the requested file; paragraph [0048] describes that the name and metadata of the file selected in the search results may not necessarily be the same as the name and metadata attached to the file by the second peer, and that the requesting peer notifies the server that it has a copy of the file to become a filling peer for a subsequent request for the same file; and paragraph [0049] describes that when the fulfilling peer is no longer online, the requesting peer will select the next location peer (peer3) from the list of available locations. And Paragraph [0034] describes that the central directory data, which includes a file directory table, may be stored in a relational database, and further describes the contents of the tables.

Nothing in the paragraphs cited by the Examiner teaches or suggests "allowing the client nodes to subscribe with the server node to periodically receive copies of one of the files... and transferring files from the closest node directly to the current subscribing node" as recited in claims 2, 17, 31, and 32. In fact, Applicant has performed a keyword search on Scott and the terms "subscription" and "subscribe" were not found. Appendix C of Scott on page 8 of 53 includes the term "Auto-Update" and page 49 of 53 includes the terms "Fileclubs", but no descriptions or definitions of the terms are provided. Therefore, it is difficult for the Applicant to ascertain whether or not the terms "Auto-Update" and "Fileclubs" are analogous to the claimed "subscription-based decentralized file downloads." In any event, even if the terms "Auto-Update" and "Fileclubs" were considered analogous to subscriptions, it is respectfully submitted that Scott's "Auto-Update" and "Fileclubs" feature are not taught in combination with a client node "generating a new fingerprint" in response to receiving a file from another client node in order to "determine the authenticity of the file and publisher," as recited in

claims 2, 17, 31, and 32. Absent any teaching or suggestion to the contrary, it is respectfully submitted that claims 2, 17, 31 and 32 are allowable over Scott and Farber.

The arguments above apply with full force and effect to the remaining dependent claims because they are based on allowable independent claims. Therefore, the dependent claims are allowable for at least the same reasons as the independent claims.

In view of the foregoing, it is submitted that claims 1-2, 7-16, and 22-32 are allowable over the cited references. Because the secondary references stand or fall with the primary references, claims are allowable because they are dependent upon the allowable independent claims. Accordingly, Applicant respectfully requests reconsideration and passage to issue of claims 1-2, 7-16, and 22-32 as now presented.

Applicants' attorney believes this application in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,

SAWYER LAW GROUP LLP

July 26, 2005
Date

Stephen G. Sullivan
Attorney for Applicant(s)
Reg. No. 38,329
(650) 493-4540